

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

UNITED STATES OF AMERICA,)	
)	
Plaintiff,)	
)	
v.)	Case No. 08-CR-201-TCK
)	
ANDRE RALPH HAYMOND,)	
)	
Defendant.)	

OPINION AND ORDER

This matter is before the Court on Defendant Andre Ralph Haymond's ("Haymond") "Supplemental" Motion to Compel (the "Supplemental Motion").¹ [Dkt. No. 36].

I.
Background

Defendant's Supplemental Motion renews his request for access to images allegedly contained on his computer that was seized by the Government pursuant to a search warrant in January 2008 and thereafter Defendant was charged with possession of child pornography. The Government made a mirror image of Defendant's computer's hard drive. For convenience, this mirrored hard drive was made available

¹ Haymond describes his motion as a "supplement" to his previous Motion to Compel [Dkt. No. 28]; however, on Aug. 28, 2009, the Court denied the previous Motion to Compel without prejudice. [Dkt. No. 35]. Therefore, Defendant's latest filing is a new motion. However, for simplicity, it will be referred to herein as the "Supplemental Motion."

to Defendant's expert, David Penrod ("Penrod") at the Regional Computer Forensic Laboratory ("RCFL") in Denver, Colo., near Penrod's home.

Initially, Penrod complained that he was unable, using his Encase software, to find any pornographic images on the mirrored hard drive. This generated Defendant's first Motion to Compel [Dkt. No. 28]. On Sept. 2, after the Court directed Penrod to return and work with the RCFL to try again to access the images, he was able to find 14,000 images on the hard drive using the Government's Forensic Tool Kit ("FTK") software. Allegedly, 78 of these images are unlawful child pornography. Defendant now complains that he cannot tell *which* of the 14,000 images are the 78 images on the hard drive that the Government contends constitute child pornography.² Defendant further complains that the images have been "stripped" of all metadata that would enable him to prepare a forensic defense to the pending charge.

II.

Applicable Legal Principles

Procedural due process requires that a criminal defendant facing potential loss of his liberty receive due notice of the charge against him and a reasonable opportunity to defend himself. *E.g., In re Oliver*, 333 U.S. 257, 273 (1948); *Powell v. State of Ala.*, 287 U.S. 45 (1932). This requires that a Defendant be given notice of the specific charge against him and a chance to be heard through a trial of the issues raised by the charge.

² There are 140 images at issue here. Of these, the Government claims to have identified 78 pornographic images on Defendant's computer hard drive and 62 images (including one video clip) that allegedly were made available through LimeWire from a location associated with Defendant. (LimeWire is a free peer-to-peer file sharing service using the Java platform.)

In furtherance of this due process right to be heard, Rule 16 of the Federal Rules of Criminal Procedure provides:

Documents and Objects. Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and:

- (i) the item is material to preparing the defense;
- (ii) the government intends to use the item in its case-in-chief at trial; or
- (iii) the item was obtained from or belongs to the defendant.

Fed.R.Crim.P. 16(E).

However, this discovery provision was modified by the Adam Walsh Act in July 2006. One provision of that Act restricts a defendant's access to discovery materials that constitute child pornography:

- (1) In any criminal proceeding, any property or material that constitutes child pornography (as defined by section 2256 of this title) shall remain in the care, custody, and control of either the Government or the court.
- (2)(A) Notwithstanding Rule 16 of the Federal Rules of Criminal Procedure, a court shall deny, in any criminal proceeding, any request by the defendant to copy, photograph, duplicate, or otherwise reproduce any property or material that constitutes child pornography (as defined by section 2256 of this title), so long as the Government makes the property or material reasonably available to the defendant.
- (B) For the purposes of subparagraph (A), property or material shall be deemed to be reasonably available to the defendant if the Government provides ample opportunity for inspection, viewing, and examination at a Government facility of the property or material by the defendant, his or her attorney, and any individual the defendant may seek to qualify to furnish expert testimony at trial.

18 U.S.C. § 3509(m).

Pursuant to this statute, a court shall deny a defendant's requests to copy or otherwise reproduce child pornography as long as the material is made "reasonably available" to the

defendant. “Reasonably available” requires the Government to provide an “ample opportunity” for inspection at a Government facility. In *U.S. v. Flinn*, 521 F.Supp.2d 1097, 1101 (E.D.Cal. 2007), the court discussed what this “ample opportunity” includes.

An ample opportunity to forensically examine seized computer items means an examination whereby the government can supply reasonably up-to-date tools (hardware and software) and facilities such that a defendant can construct a reasonable, available forensic defense, if one is available at all, and whereby the analysis will not be impeached because it was not supported by the proper hardware or software. An ample opportunity will permit a defense expert to utilize his or her hardware or software. An ample opportunity also requires that the analysis be performed in a situation where attorney-client privilege and work product will not be easily, accidentally exposed to the government, and in a facility which is open to the defense at its request during normal working hours, and to the extent feasible, during non-working hours.

Id.

III. *Discussion*

Haymond was indicted on Dec. 8, 2008 for an alleged violation of 18 U.S.C. §§ 2252(a)(4)(B) and 2252(b)(2). The Indictment charges that Haymond knowingly possessed child pornography “including, but not limited to” five specific files.³ The Government has since described a total of 140 pornographic images at issue. See footnote no. 2, *supra*.

³ The files are named:
 JPEG_6578176[148934].jpg;
 JPEG_13484032[149950].jpg;
 JPEG_17362944[149185].jpg;
 JPEG_7811072[150568].jpg;
 JPEG_14241792[149794].jpg.

[Dkt. No. 2].

These 140 images have been made available to Defendant's counsel at the office of the United States Attorney in Tulsa. Additionally, a mirror-image of the hard drive from Defendant's computer has been sent to the RCFL in Denver for easier access by Penrod. Defendant complains that in spite of his expert's efforts, he has been unable to locate the 78 images on the mirrored hard drive that the Government contends constitute child pornography.

The Court has two fundamental concerns with the discovery situation as it has been presented. First, ensuring that Defendant receives reasonable access to discovery that will permit him to contest the charge(s) against him. Second, seeing that discovery is concluded efficiently so that the trial of this case may proceed without needless interruption. Defendant is entitled to certain discovery pursuant to Fed. R. Crim. P. 16; however, the Adam Walsh Act places certain restrictions on discovery available to a Defendant in a child pornography case. The intersection of Rule 16 and the Walsh Act is a frequent discovery battleground in these cases. Material constituting child pornography must remain in the possession of the Government or the Court; thus, the Defense does not have the same Rule 16 right to copy this material as it does non-pornographic material. Instead, the Defendant, his lawyer and expert must be given an "ample opportunity" to inspect the material at a Government-controlled facility.

Defendant has raised three issues concerning discovery. These are each addressed below.

(A) 'Missing' Metadata.

Defendant says he is unable to find any metadata associated with the files on the mirrored hard drive and implies that the Government may have “stripped” this metadata when it “data carved” images from the hard drive.⁴ The Court rejects Defendant’s implication that metadata was removed from the hard drive by the Government. At the hearing on Sept. 16, 2009, the Government stated that the hard drive provided to Defendant was a “complete, exact” copy of the hard drive the Government accessed and that if Defendant did not have metadata, it is because the metadata is simply not there.⁵ Furthermore, Defendant’s own expert, Penrod, represented to the Court at the Aug. 24 hearing that he did not expect and was not looking for metadata. The Court has reviewed the tape of that hearing in detail. At the Aug. 24 hearing, the Court specifically asked Penrod if he was seeking metadata on the mirrored hard drive. He replied:

Metadata is simply data such as the logical path to a file and the date and time of creation. Those kinds of things. And you’re not going to find that with any kind of -- or with about 95 percent of data-carved items. All you’re going to get is the image in this particular situation and the physical location of where that data is actually located on the hard drive.

⁴ “Data-carving” or harvesting is the process of retrieving electronically stored information from storage media or devices. Shira A. Scheindlin, Daniel J. Capra, *Electronic Discovery and Digital Evidence*, at 681-82 (West 2009). The process generally relies on a search based on file content, rather than metadata. See http://www.forensicswiki.org/wiki/File_Carving (accessed Sept. 16, 2009).

⁵ The Court has pointed out that in previous filings counsel has stated that Defendant routinely “nuked” his computer to remove “everything that had accumulated on the hard drive.” [Dkt. No. 28 at 2]. The Court is left to wonder what effect this “nuking” had on data remaining on the hard drive.

Later when Defense counsel queried Penrod about getting metadata for use in preparing a defense, Penrod stated that he was “99.99-percent sure we won’t find any metadata associated with these files.” Given Penrod’s statements, the Government’s representations at the Sept. 16 hearing, and the lack of any evidence to suggest that the Government “stripped” metadata from the hard drive before creating the mirror-image hard drive, the Court finds no basis for Defendant’s complaint in this regard.

(B) Locating images on the mirrored hard drive.

Defendant complains that he cannot find the 78 images that the Government contends are on the mirrored hard drive without poring over all 14,000 images found there. At the Sept. 16 hearing, the Government agreed to send to the RCFL CDs containing all 140 images at issue in this case. These will be made available to Penrod at the RCFL and will remain in the custody and possession of the Government. Penrod will be able to access these images and compare them to data on the mirrored hard drive. Defense counsel stated that this will obviate the need for any cluster/sector information to locate the images as he had previously requested.

(C) Redacted Images for Subpoenas.

Defendant wants the Government to prepare redacted copies of the images at issue so that he can use them with subpoenas to the internet web sites where the images originated. Defendant plans to subpoena information from the web site owner to the effect that the persons portrayed in the pornographic images are adults, not minors. At the Sept. 16 hearing, the Government stated that the core of its case at trial will be based on 10-12 of the 140 images. These include one video file and photographs where the

Government has identified a juvenile victim. These images have been identified in the Child Victim Identification Program (“CVIP”) report available to Defendant. While the Government has not absolutely restricted itself to only using these 10-12 images at trial, it has confirmed that these will be the central core of the case. Additionally, Defense counsel has estimated that only about 15 percent of the images he has reviewed have any web site information embedded in them that would provide a basis for a subpoena. Accordingly, Defendant should focus on the 10-12 images identified in the CVIP report. If there are images with embedded web site information that Defendant wants to subpoena, he shall identify those files well before trial and the Government will prepare redacted images for his use.⁶

IV. *Conclusion*

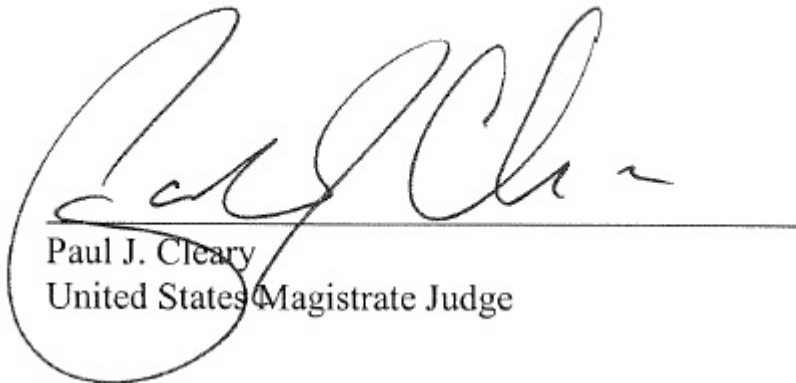
Due process and judicial economy require both sides have a reasonable understanding before trial as to the specific material that forms the basis of the Government’s substantive charge and what such material the Government intends to present to a jury. Trial of this case has been continued four times; any further disruption of the trial must be avoided.

Accordingly, within 10 days of the date herein, the Government shall provide CDs containing all 140 images allegedly containing child pornography. These will be sent to the RCFL and maintained under the Government’s control just as the mirrored

⁶ Apparently, this is the procedure that was used in *U.S. v. Terry Brian Dobbs*, Case No. 07-CR-149-GKF. However, Defense counsel conceded at the Sept. 16 hearing that the subpoena issued in *Dobbs* to an internet site in Holland resulted in a “wild goose chase.” That is, it was ignored by the subpoena recipient.

hard drive is maintained. The defense shall be given reasonable access to the CDs and the mirrored hard drive at the RCFL and an ample opportunity to examine both. If Defendant identifies specific images with embedded internet site information, and upon reasonable notice to the Government, the Government will prepare redacted copies of those images for Defendant's use in conjunction with subpoenas to the web sites. Defense counsel is cautioned, however, that given the lack of results from the subpoena effort in *Dobbs*, such a request should be narrowly tailored in a reasonable effort to secure material information.

It is so ordered this 16th day of September 2009.



Paul J. Cleary
United States Magistrate Judge